IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (Currently Amended) A packet filtering method characterized by storing filtering information for use in filtering at a receiving side in an encrypted packet to be sent to the receiving side and sending it from a sending side, wherein

an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information as to prevent the filtering information from being encrypted when the packet is a packet in compliance with Ipv6, wherein said filtering information is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

2. (Currently Amended) A packet filtering method characterized by receiving an encrypted packet, at a receiving side, from a sending side, detecting filtering information stored in that packet, holding predetermined filtering information of the receiving side, comparing filtering information of the sending side detected from the packet with the filtering information of the receiving side, and, when the two do not match, discarding that packet, wherein an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6, wherein said filtering information is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

3. (Currently Amended) Communication equipment at a packet sending side including a function unit for achieving a packet filtering,

said communication equipment characterized by having at least:

a setting unit for setting filtering information,

a filter key holding unit for holding the filtering information input by the setting unit as a filter key, and

a filter key storing function unit for receiving as input the held filter key and storing the filter key in a header portion of an encrypted packet, wherein

an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6, wherein said filtering information is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

4. (Currently Amended) Communication equipment of a packet receiving side including a function unit for packet filtering, said communication equipment characterized by being provided with:

a filter key detecting unit for receiving an encrypted packet sent from a sending side while storing information as a filter key in a header portion of the packet and detecting the filter key from the header portion; and

a comparing function unit for comparing a filter key of a sending side detected by the filter key detecting unit with a filter key of the receiving side held in advance, determining if the two do not match, and, when they do not match, discarding the received packet, wherein

an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6, wherein said filtering key is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

5. (Previously Presented) Communication equipment as set forth in claim 4, characterized in that:

the equipment is provided with a buffer for temporarily storing a received packet passing through the filter key detecting unit and in that the comparing function unit is comprised of:

a filter key table holding a predetermined plurality of different filter keys,

a search unit for searching if there is a filter key matching with a filter key detected by the filter key detecting unit in the filter key table and when there is none, outputting a discard

command, and

a buffer control unit for receiving the discard command and controlling the system so as to discard the packet stored in the buffer.

6. (Cancelled)

7. (Cancelled)

8. (Currently Amended) A packet communication system where a transferred packet is filtered, said packet communication system characterized by being provided with:

a packet transmitting apparatus for storing filtering information for use in filtering at a receiving side in a packet to be sent to the receiving side and sending it from a sending side,

a packet receiving apparatus for receiving an encrypted packet, at the receiving side, from the sending side through a network between a server and client, detecting filtering information stored in the received packet, holding predetermined filtering information of the receiving side, comparing filtering information of the sending side detected from the packet with the filtering information of the receiving side, and, when the two do not match, discarding that packet, and

an authentication apparatus for receiving user authentication information input from a user receiving filtering service, authenticating the user, and assigning and distributing a filter key as filtering information corresponding to the user authentication information to the user after the authentication, wherein

an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6, wherein said filtering information is used for identifying a specific value showing a VoIP performing VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

9. (Currently Amended) A packet communication system where a filtering service is provided for an encrypted packet transferred through a network between a server and a client, the packet communication system characterized by being provided with:

function units used for access from the server or client of the user side to the network, that is, a first function unit for receiving user authentication information and authenticating the

user and

a second function unit for restricting access by assigning and distributing a filter key as filtering information corresponding to the user authentication information to the user after the authentication, wherein

an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6, wherein said filtering key is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

10. (Currently Amended) A packet communication system where a filtering service is provided for an encrypted packet transferred through a network between a server and a client, the packet communication system characterized by being provided with:

function units used for access from a user on a network side to the server or client, that is,

a first function unit for receiving user authentication information and authenticating the user and

a second function unit for restricting access by assigning and distributing a filter key as filtering information corresponding to the user authentication information to the user after the authentication, wherein

when the packet is a packet in compliance with Ipv6,an IPv6 extended header added to an IPv6 header or in a flow label region in an IPv6 header is used to transmit the filtering information so as to prevent the filtering information from being encrypted, wherein said filtering information/filtering key is used for identifying a specific value showing a VoIP performing a VoIP communication, and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously.

11. (Cancelled)

12. (Previously Presented) A communication equipment as set forth in claim 4, wherein an authentication apparatus is further included, the authentication apparatus having:

a filtering authentication function unit for receiving user authentication information input from a user receiving a filtering service and authenticating the user; and

a filter key providing function unit for assigning and distributing said filter key to be stored in a packet corresponding to the user authentication information to the user after the authentication at the filtering authentication function unit.

13. (Currently Amended) A communication equipment as set forth in claim 12, wherein said filtering authentication function unit has:

a user authentication database in which user authentication information is registered in advance, and

a decision unit for determining the veracity of the input user authentication information by referring to the user authentication database; and

said filter key providing function unit has:

a filter key assigning table holding said filter key assigned in advance corresponding to user authentication information, and

a filter key sending unit for sending a corresponding filter key from the filter key assigning table to the user when the veracity is confirmed, wherein said filtering information is used for identifying the specific value showing the VoIP performing the VoIP communication, the specific value showing the VoIP provides a first function of the filtering and a second function of having the communication partner recognize the VoIP, simultaneously.

14. (Currently Amended) A method, comprising:

storing filtering information in an extended header of an encrypted packet ~~incompliance~~ in compliance with IPv6 to prevent the information from being encrypted~~, the information indicating that a communication is over VoIP~~; and

transmitting, to the receiving side, the encrypted packet with the filtering information to enable filtering of [[the]]a VoIP communication, wherein the filtering information includes a specific filtering value to filter the VoIP communication and allows a communication partner to recognize the VoIP communication, simultaneously.